PARADIGMAVÁLTÁS – BIZTONSÁG – EMBERI TÉNYEZŐ

PARADIGM SHIFT – SECURITY – HUMAN FACTOR

KESZTHELYI ANDRÁS LÁSZLÓ egyetemi docens
Óbudai Egyetem, Keleti Károly Gazdasági Kar

ABSTRACT

Nowadays we experience a paradigm shift because of the computers and networking having become part of our everyday life. Most of the rules and procedures we have been accustomed to for centuries will never work in the future. This is why, for example, music downloading and in some cases even the seeding have been made legal in Hungary. The paradigm shift, caused by the digital technology, has a strong effect on the field of information security as well. Our age might be called as the age of cybercrime and cyber warfare if we look at the collection of security incidents in the past one and a half decade. In such a situation the role of the human factor becomes more and more important, including, but not limited to, teaching and learning.

1. Paradigma, paradigmaváltás

Az idegen szavak szótára szerint: paradigmatikus gör – lat 1. mintaszerű, szabályszerű (...) (Bakos, 1989.). Hétköznapi szóhasználat szerint valamely közösségnek adott korszakban általánosan elfogadott, axiómaszerű nézet- és szabályrendszere, amelynek megkérdőjelezése a közösségből való kirekesztéssel jár. „Ezeken olyan, általánosan elismert tudományos eredményeket értek, amelyek egy bizonyos időszakban a tudományos kutatók egy közössége számára problémáik és problémamegoldásaik modelljeként szolgálnak.” (Kuhn, 1984, p. 11.) A történelem kezdeteitől mindmáig az élet számos, ha nem minden területén megfigyelhetők a paradigmák. Gondoljunk csak napjaink „politikai korrektség” fogalmára, vagy arra, amikor 2011-ben a CERN és a Gran Sasso Laboratórium – úgy tűnt – a fénysebességnél gyorsabb részecskesebességet mért.

Paradigmaváltásról akkor beszélhetünk, amikor ez a nézet- és szabályrendszer valamilyen okból hirtelen, rövid idő alatt megváltozik. Ez az ok többféle lehet. A tudomány világában például új eredmények, felfedezések válthatják ki. A közéleti-társadalmi paradigmaváltást gyakran forradalmak vagy – többnyire vesztes – háborúk eredményezik. Előfordul azonban az, hogy új technológia megjelenése és elterjedése eredményezi ezt.

Jó ötszáz évvel ezelőtt Gutenberg feltalálta – Európában – a könyvnyomtatást, evvel a könyvek sokszorosítását ipari folyamattá változtatta: a korábbiakhoz képest töredék idő alatt és közel korlátlan példányszámot lehetett előállítani. Ennek két fontos következménye lett. Egyrészt megszűntek a kódexmásoló szerzetesi műhelyek, ami kétségtelen veszteség. Másrészt azonban a tudás továbbadása és raktározása sokkal hatékonyabbá vált, olyannyira, hogy az írásbeliség kizárólagossá vált és maradt fél évezred óta. Igaz, a papír egyre drágább, az elkészült könyvek raktározása és szállítása drága és nehézkes, az egyszer már elkészült könyvek utólagos másolhatósága korlátozott. Ugyanez igaz az analóg zene (bakelit lemez, kazetta) és film (celluloid szalag) esetére is.

2. A digitális hálózatok paradigmaváltása

Napjainkban hasonló, sőt talán még nagyobb hatású paradigmaváltás zajlik. Az 1990-es évek elejére a személyi számítógépek és a hálózat elterjedésének általánossá válása indította el ezt a folyamatot. 1989-ben a CERN-ben Tim Berners-Lee vezetésével elkezdik a ma világháló néven ismert új hálózati szolgáltatás (html, hiperszöveges jelölő nyelv és http protokoll) kidolgozását, 1993-ban pedig közkinccsé tették, (CERN, 2014.) s a gopher fizetőssé válása után egyeduralkodóvá vált a digitális tartalmak közvetítése terén. A számítási teljesítmények gyors növekedése lehetővé tette a hatékony digitalizálást, nemcsak a szöveges tartalmak, de a zene és a film világában is.

A közismert következmények: gyakorlatilag nulla idő alatt tetszőleges számú másolat készíthető, a másolás és a használat során minőségvesztés (kopás) nem lép föl. A digitális-virtuális síkra való átlépéssel a fizikai gyártási költség (nyomda, lemez-, kazettagyártás) megszűnik, hasonlóképpen a világ(háló) bármely pontjára való eljuttatás költsége is elenyészik.

További következmény, minőségi újdonság, hogy a tartalmak gépi úton kereshetővé váltak. Van Google és működik – szöveges tartalmaknál legalábbis – a „Ctrl-F".

A tudás átadására és megszerzésére sosem voltak ennyire könnyű lehetőségeink a történelem folyamán, mint napjainkban. A mérleg másik serpenyőjében pedig egyfajta veszteség van – hasonlóan a kódexmásoló műhelyek valamikori helyzetéhez –, a könyv- és zeneműkiadók egy része, esetlege jelentős része meg fog szűnni. Van azonban az új helyzetnek más – aggasztóbb – következménye is.

3. Az új paradigma sajátos következményei

Az új technológia következménye, hogy korábban soha nem látott módon megnövekedett a – virtuális világbeli – bűnözés, kémkedés, ipari kémkedés, sőt háborúzás mennyisége, súlyossága és gyakorisága, és az egyes területek közötti határvonalak elmosódnak. Az új paradigma sajátosságai közé tartozik, hogy a hagyományos fogalmak többé nem használhatók.

Ha a kocsim ott áll, ahol hagytam, akkor azt egyértelműen nem lopták el. Ha bejelentkezem a számítógépembe, és adataimat rendjén megtalálom, abból még nem következik, hogy azokat nem lopták el, már régen, akár sokszor is. A PC architektúra sajátosságaiból következik, hogy a gép őrizetlenül hagyása, illetve hálózatra való csatlakoztatása után nincs garancia arra, hogy csak a gazdájának van hozzáférése. A virtuális világban fokozottan igaz, hogy az ügyfél nem biztos, hogy az, akinek kiadja magát (l. Stavridis tengernagy esete). További komoly különbség, hogy míg egy kocsilopásnál a tettes személyesen jelen van a lopás helyszínén és időpontjában, addig a virtuális világbeli akciók esetében – legyen szó adatlopásról vagy bármi másról – a tettesnek sehol és semmikor nem kell szükségszerűen ott lennie. Egy hagyományos bomba leesik, felrobban, pusztít, és vége. A „virtuális bomba", példának okáért a Stuxnet vírus bejut, pusztít, de végül nemcsak felfedezik, hanem elemzik, többé-kevésbé átalakítják, és újrahasznosítják, akár eredeti kifejlesztői ellen is (l. Stuxnet). Az Internet formálisan is hadszíntérré vált (l. Robert Elder).

Mindezek után az új korszak komoly problémái:

- Észleled-e egyáltalán a biztonsági incidens tényét? (l. Kennedy Űrközpont és az Uroburos kémprogram)
- Ha igen, megállapítható a tettes?
- Ha igen, bizonyítható is?
- Vajon a törvény képes megvédeni?

A tettes megállapíthatóságának és a bizonyíthatóságnak a problémái következnek abból, hogy ha sikerül megállapítani, hogy milyen IP-címre távoztak adataink, abból még nem következik, hogy az adott gép gazdája azonos az elkövetővel, hogy az adott gép nem pusztán a nyomok elrejtésére szolgáló köztes állomás volt. Esetenként még a cél is kérdéses lehet (l. a tőzsdei példa).

A helyzet súlyosságát talán a legjobban a Websense megállapítása példázza: „A kérdés nem az, hogy meghekkelnek-e, hanem hogy mikor." (Websense, 2011)

A röviden vázolt helyzetben jogosnak látszik a következtetés: a westernfilmek vadnyugatának virtuális párján élünk, és csak magunkat védhetjük meg. Akár magányszemélyként, akár kis-, közép- vagy nagyvállalatként. Törvény ugyan van, de a seriffre hiába is várnánk. A jogászok különben is avval vannak elfoglalva, hogy megkíséreljék a klasszikus katonai fogalmakat a virtuális hadszíntérre átértelmezni (Schmitt, 2013) (Bodnár, 2013). Hogy mennyire sikeresen, azt majd az idő fogja (vagy nem fogja) megmutatni. Addig is zajlik a világhálón a harmadik világháború (Hanula, 2013) (Portfolio, 2013) (l. Robert Elder, lennebb).

4. Példák

A példákat szinte a végtelenségig lehetne sorolni. Az ismertté vált jelentősebb incidensek sora ijesztő képet rajzol elénk. Nincs az életnek olyan területe, ahol ne állna fenn a veszélyhelyzet – nemcsak a digitálisan, számítógépeken tárolt adatok

mennyisége növekszik napról-napra, de az ezektől való függésünk is. Lehet manipulálni katonai repülőt (MTI, 2011), utasszállító repülőgépet (Teso, 2013), kocsit (Kosher, 2010) (Checkoway, 2011), szívritmusszabályozót (Index, 2012).

Lássunk csak néhány példát, illusztrációképpen, tanulságul.

- 2005 áprilisában „kiberbetörők" sikeresen behatoltak a NASA Kennedy Űrközpontja különlegesen biztonságos (illetve annak tartott) hálózatába, és sikeresen telepítettek egy kémprogramot (stame.exe), ami meghatározatlan mennyiségű adatot küldött az űrsikló(k)ról tajvani számítógépekre, vagy azokon keresztül valahova máshova. Az ellopott adatok mennyisége legalább 20 GB, tömörítetten. Az adat„szivárgást" csak fél évvel később, novemberben fedezték föl. (Epstein, 2008)
- Robert Elder Jr. háromcsillagos tábornokot nevezték ki az USA első kibertábornokává. Az alakulat megalakulásakor tervezett létszáma húszezer fő, programozók, mérnökök, az elektronikus hadviselés szakemberei. Az alakulat tevékenysége kiterjed az adatok számítógépes hálózatokon való tárolásának, módosításának, forgalmazásának és a kapcsolódó hardvernek az elektronika és az elektromágnesesség teljes területére. (Carrol, 2008)
- A Stuxnet vírus tönkretette véletlenszerűen hibás vezérlési utasításokat adva ki az urándúsító centrifugák egy részét Iránban. Becslések szerint az akció akár két évvel is hátráltathatta az iráni atomprogramot. 2010 végén a Stuxnetet tartották a legagresszívabb és legfejlettebb kártékony programnak biztonságtechnikai szakértők. A vírus hatékonysága, illetve az a körülmény, hogy különleges, ipari számítógépeket támadott, és hatékonyan tudta manipulálni az ezek által vezérelt atomcentrifugákat, azt mutatja, hogy Izrael és az Amerikai Egyesül Államok állt a fejlesztés hátterében. Egyes vélemények szerint ezt az eseményt tekinthetjük a kiberháború kezdetének. A programot egy kettős ügynök juttatta be usb-kulcson a külvilágtól elszigetelt belső hálózatra. (Chen, 2010) (Cluley, 2012) (Vaas 2013) A későbbiek folyamán a Stuxnetben rejlő innovációt más célokra is kihasználták, több átalakított változata is elterjedt a (nyugati) világban, ilyen pl. a Duqu. (Bencsáth, 2012).
- Az emberi tényező szerepének „szép" példája. Feltehetően kínaiak a Facebook segítségével szerezték meg sikeresen NATO-alkalmazottak személyes adatait. Előbb létrehoztak egy hamis profilt James Stavridis tengernagynak, a NATO európai főparancsnokának a fényképével és adataival, majd nevében ismerősnek jelölték kollégáit, akik közül azt számosan elfogadták, hozzáférhetővé téve így adataikat a profil igazi üzemeltetői számára. (Hopkins, 2012)
- Az amerikai tőzsdén egy rövid ideig a kötések 4%-át egyetlen program generálta. 25 ezredmásodpercenként küldött megbízás-csomagokat 200-1000 darab megbízással csomagonként, és ezeket azonnal vissza is vonta. A szakértők szerint feltehetően tesztelés zajlott. Így is igen komoly aggodalmak merülhetnek föl, hiszen az online tőzsdei rendszer manipulálását, akár teljes megbénítását sem lehet kizárni egy ilyen módszer esetén. (Melloy, 2012)

– 2014 tavaszán az Egyesül Államok kormányzati szerveinek számítógépein fölfedeztek egy rendkívül fejlett kémprogramot, az Uroburost, amely bizalmas adatokat továbbított. A programot feltehetően oroszok fejlesztették, és az adatokat feltehetően orosz számítógépekre továbbította. Egyik érdekessége, hogy feltehetően évek óta működött észrevétlenül. Ennek egy elődje úgy jutott be az amerikai Védelmi Minisztérium rendszerébe, hogy egy fertőzött usb-kulcsot talált egy alkalmazott a parkolóban... (GData, 2014) (Vírusirtó, 2014).

5. Mit tehetünk?

Mivel a személyes, fizikai jelenlét nem szükségszerű követelménye a különféle netes cselekményeknek a közönséges lopástól a háborús cselekményekig, ami a személyes kockázat elfogadható szintre való csökkentését jelenti. Ezért teljesen logikus a területen jelenleg is meglévő, és várhatóan erősen fokozódó egyéni aktivitás, sőt az állami szerepvállalás is. Ugyanis „A kiberhadviselés két ok miatt került előtérbe az utóbbi hónapokban – és igazából az a meglepő, hogy a vírusok és hekkerek hatalmas előnyét a tankokhoz és bombákhoz képest csak mostanában kezdik kihasználni az egyes országok hadseregei. Az egyik ütőkártya az, hogy az online háborúzás a támadó oldalán relatíve olcsó, az okozott károk ehhez képest aránytalanul, sok nagyságrenddel magasabbak, a védelem kiépítése pedig iszonyatos összegeket emészt fel. Ezt a hadtudomány asszimetrikus [sic!] hadviselés néven ismeri, ebbe a kategóriába sorolja például a terrorizmust és a gerillahadviselést is.” (Hanula, 2013)

Mit tehetünk ilyen helyzetben, magánemberként és vállalkozásként? Nyilvánvalóan, axiómaszerűen alkalmazzuk a fizikai, ügyviteli és algoritmusos védelem rendelkezésre álló technikáit és technológiáit, a mindenkori iparági legjobb gyakorlatnak megfelelően. Ha nem így tennénk, az súlyos felelőtlenség volna. Még akkor is, ha a fenti példák alapján jogosan merül föl a gondolat, miszerint ezek messze vannak a tökéletestől. Éppen ezért, ugyancsak nyilvánvalóan, további lépésekre is szükség van.

Mivel a világhírű víruskeresők sem voltak képesek – nyilván különböző okokból – kimutatni egyes kártevőket, a Sony rootkittől (Schneier, 2005) az Uroburosig, a védekezés technikai oldalát erősíteni szükséges, és elsősorban egyedi megoldásokkal. A szabványos, ipari, ismert megoldásokat ugyanis az ellenérdekelt felek is jól ismerik, azok kikerülésére fel tudnak készülni.

Közhelyszerű megállapítás, hogy minden biztonsági rendszer leggyöngébb láncszeme az ember (l. a Stuxnet és az Uroburos példáját is). Ennek kézenfekvő következménye, hogy az emberi tényező fejlesztése a másik szükséges lépés. Emiatt felértékelődik az oktatás, képzés, továbbképzés, gyakorlás és motiváció szerepe és jelentősége. Az alkalmazottak céges továbbképzése – egyelőre – adómentes természetbeni juttatás is, és a vállalkozás elemi önvédelmi érdeke. Mert hiába a gon-

dosan összeállított szabályzatok, minél kevesebbet értenek belőle (és a hátteréből) az alkalmazottak, annál kevésbé lesznek érdekeltek a gondos betartásukban. Ezen, emberi erőforrás alapú megközelítés még tovább fejleszthető (Benke, 2014) a biztonsági kultúra irányába. (Lazányi, 2014).

Ezen túl pedig a terület olyan gyorsan változik, hogy a mai tudás – ha egyáltalán megvan – holnapra már elavulttá válhat. Felértékeli a továbbképzések jelentőségét, ha az alaptudás messze van az elvárható ideálistól. Magyarországon és Közép-Európában pedig, sajnos, ez utóbbi a helyzet. (Kiss, 2011) (Kiss, 2012)

„Egy lovag egyszer nem igazította meg lova egyik patkójában a patkószeget. A patkószeg miatt a patkó elveszett. A patkó miatt ló elveszett. A ló miatt a lovag elveszett. A lovag miatt a csata elveszett. A csata miatt a hadjárat elveszett. A hadjárat miatt az ország is elveszett. Igazítsd meg rendesen a patkószöget!”

FELHASZNÁLT IRODALOM

Az online tartalmak elérhetősége 2014. május 20. és 28. között fennállt, ahol ettől eltérő jelzés nincs.

Bakos Ferenc (szerk.) (1989). Idegen szavak és kifejezések szótára, Akadémiai Kiadó, Budapest

Bencsáth, B. et al. (2012). Targeted attacks against Critical infrastructure: Stuxnet and beyond, SCADA and Smart Grid Cyber Security Summit, 26-27 April 2012, April, 2012, London

Benke, M. (2014). Az emberi tőke „készletezési” problémáinak változó jellege, VIKEK, megjelenés alatt

Bodnár, Á. (2013). Elkészült a NATO kibervédelmi kézikönyve, HWSW Online Informatikai Hírmagazin, http://www.hwsw.hu/hirek/49922/tallinn-manual-informatikai-hadvieles-nato-biztonsag-krasznay-csaba.html

Carrol, W. (2008). The New Cyber General, http://defensetech.org/2008/01/02/the-new-cyber-general/

CERN (szerk.) (2014). The birth of the web, http://home.web.cern.ch/topics/birth-web

Checkoway et al. (2011). Comprehensive Experimental Analyse of Automative Attack Surfaces, USENIX Security, 2011.08.10-12. http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Chen, T. M. (2010). Stuxnet, reh Real Start of Cyber Warfare?, IEEE Network, Nov/Dec 2010, pp. 2-3.

Cluley, G. (2012). Stuxnet: How USA and Israel created anti-Iran virus, and then lost control of it, http://nakedsecurity.sophos.com/2012/06/01/stuxnet-usa-israel-iran-virus/

Epstein, K. (2008). Network Security Breaches Plague NASA, Bloomberg Businessweek Magazine, http://www.businessweek.com/stories/2008-11-19/network-security-breaches-plague-nasa

GData (szerk.) (2014). Uroburos Highly complex espionage software with Russian roots, GData Red Paper, https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

Haunla, Zs. (2013). A neten már zajlik a harmadik világháború, Index, http://index.hu/tech/2013/05/06/a_neten_mar_zajlik_a_harmadik_vilaghaboru/

Hopkins, N. (2012), China suspected of Facebook attack on Nato’s supreme allied commander, The Guardian, http://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato

Index (szerk.) (2012). Tömeggyilkoságot is el lehet követni a pacemakerek hekkelésével, http://index.hu/tech/2012/10/19/tomeggyilkossagot_kovethet_el_a_pacemakerhekker/

Kiss, G., 2012. Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course. TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4., pp. 222-235. Oct. 2012.

Kiss, G., 2012. Measuring Hungarian and Slovakian Students' IT Skills and Programming Knowledge. Acta Polytechnica Hungarica, Volume 9., No. 6, 2012, ISSN: 1785-8860, pp. 195-210.

Koscher et al. (2010). Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy, Oakland, CA, 2010.05.16-19. http://www.autosec.org/pubs/cars-oakland2010.pdf

Kuhn, Thomas (1984). A tudományos forradalmak szerkezete. Gondolat Kiadó, Budapest

Lazányi, K. (2014). A biztonsági kultúra, VIKEK, megjelenés alatt.

Melloy, J. (2012). Mysterious Algorithm Was 4% of Trading Activity Last Week, CNBC, http://www.cnbc.com/id/49333454

MTI (2011). A CIA drón földre kényszerítésének krónikája. Bombahírek, 2011.12.16. http://www.bombahirek.hu/tudomany-technika/haditechnika/20111216-a-cia-dron-foldre-kenyszeritesenek-kronikaja, letöltés: 2012.02.08.

Portfolio.hu (szerk.) (2013). A kiberháború nem vicc: Kína 30 ezer fős kiberhadsereget tart fenn, http://www.portfolio.hu/vallalatok/it/a_kiberhaboru_nem_vicc_kina_30_ezer_fos_kiberhadsereget_tart_fenn.189389.html

Schmitt, M. N. (ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press

Schneier, B. (2005). Sony's DRM Rootkit: The Real Story, https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

Teso, Hugo (2013). Aircraft Hacking. Practical Aero Series, n.runs Professionals – Security Research Team, http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20-Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf

Vaas, L. (2013). Retired, top-ranking US military officer is now Stuxnet leak suspect, http://nakedsecurity.sophos.com/2013/07/01/retired-top-ranking-us-military-officer-is-now-stuxnet-leak-suspect

Vírusirtó (szerk.) (2014). Katonai adatokra vadászik az Uroburos orosz kémprogram. http://virusirto.hu/hirek/sajtokozlemenyek/2014/03/03/katonai-adatokra-vadaszik-az-uroburos-orosz-kemprogram

Websense (szerk.) (2011). It is no longer a question of ‚if' but ‚when'! http://view.websense-email.com/view_email.aspx?j=fe5815727d6200787d11, letöltés 2011.05.24.